JIE - Transforming the Nature of Identity and Access Management (IdAM)

Our Nation's global dominance over Intelligence and Defense missions is highly reliant on the secure sharing of the most accurate and timely data available. To ensure this, the Department of Defense (DoD) Joint Information Environment (JIE) strives to deliver data securely to our warfighters wherever and whenever they need it. Since the DoD has determined cyberspace to be the new fighting domain, it must be architected and provisioned to be a collaborative, adaptable environment to effectively conduct critical operations. Additionally, this must be achieved in a fiscal climate demanding reduced Information Technology (IT) Infrastructure costs.

Based on NSA's experience with Intelligence Community Information Technology Environment (IC ITE) activities and other Smart Data initiatives, the NSA JIE Identity and Access Management (IdAM) Team identified three holistic principles that work together to increase productivity and security to ensure data protection:

- Data Tagging
- Identity and Access Management (IdAM)
- Digital Policy Management (DPM)

The focus of this article is IdAM and its role in Data Protection. IdAM is composed of three basic parts: (1) establishing an entity's identity and issuing credentials; (2) authenticating the entity; and, (3) making an authorization decision based on the known facts about the entity and the resource and the policy for access to the resource. IdAM is fundamental to the protection of data across the Enterprise and will enable secure information sharing across the cyber domain.

To achieve this end state, architects and engineers supporting JIE must develop the answer to this critically important challenge: How do we ensure that the appropriate data gets to the correct person and only to that person?

Within IT systems, access control has traditionally been enforced and managed through manually intensive, inconsistent, and time-consuming processes, many of which could pose cyber-related risks (i.e., maintaining locally administered Access Control Lists (ACLs)).

JIE IdAM is not a single process or a single technology, but is made up of a complex set of components that operate under varying policies and organizations. Progress is being made in the adoption of more automated attribute-based access control methods. In the JIE IdAM construct, JIE entities will have identities generated and be assigned enterprise entity attributes and credentials. Authentication will be predominately credential-based and implemented for every resource; authorization will host finer grained access control solutions using attribute-based techniques at all levels - Enterprise-wide, Across Communities of Interest (COI), and Regional and/or Local Sites.

As the JIE becomes the lynch-pin of the next classified cloud, the need for data tagging and granular access control becomes a major driver. The JIE IdAM Integrated Design Team (IDT) will be working in concert with the JIE Data Tagging IDT to coordinate with data and mission owners to ensure that the

data attributes produced are interoperable with JIE IdAM solutions. JIE IdAM needs to ensure that data tags are a part of the overall IdAM data used in access control decisions. All data and other resources must be protected by IdAM solutions.

The JIE IdAM IDT's efforts will be challenging in that JIE IdAM is a federated architecture where each Combatant Command/ Service/ Agency (CC/S/A) may be running its own IdAM solution. This approach is very different from IC ITE where one IdAM solution will be used. In DoD, these existing architectures and solutions will necessitate compliance with the JIE IdAM Solution Architecture and other JIE design documents. Current IdAM solutions will need to be migrated, or modified to meet the JIE IdAM compliance criteria. Additionally, the DoD Enterprise operates across a broad, geographically diverse collection of systems, nodes, and networks. Adopting and implementing IdAM solutions that work in the environment where the data resides—including Enterprise, COI, Site and the Tactical, Disconnected, Intermittent, Limited Bandwidth (TAC-DIL) environments—will present its own set of unique challenges.

As the security advisor for JIE, IAD is harnessing expertise of the United States Government to include the broader National Security Agency, DoD Commands and Services (military), and other Intelligence Community (IC) partners to craft a comprehensive data protection strategy. In addition, JIE is working to drive IT efficiencies across the DoD while enabling greater capabilities to share and protect information. JIE IdAM must orchestrate system and data access for all users and Mission Partners.